Journal of Engineering and Applied Sciences 12 (Special Issue 10): 8886-8890, 2017
ISSN: 1816-949X
© Medwell Journals, 2017

Quantum Block Encryption Algorithm Based on Unitary Operator of Pauli Matrices

Alharith A. Abdullah
College of Information Technology, University of Babylon, 51002 Hillah, Babil, Iraq

Abstract: In this study, the idea of unitary operator of Pauli matrices is employed in a new algorithm. One of the most attractive properties of this algorithm is that, we can decide when to change the operations of the algorithm whenever it is statistically necessary. The underlying operations in this algorithm are unitary operators of Pauli matrices which can be represented by using rotation matrices. The researcher divided the combination of the Pauli matrices into three groups where we perform the operation ($\mathbb{I}$, σ_x, σ_y and σ_z) in each group. Using developed encryption algorithm could encrypt the message, being transmitted over an insecure channel. The keys are created using a BB84 protocol where we require two keys K_0K_1 to encrypt a qubit and this is important in order to hide all information in all possible bases the qubit could be in. The security analysis and an example illustrating how the algorithm works are presented in this study. An overview of the complete process from the generation of the algorithm to the decryption of the message is illustrated explicitly.

Key words: Quantum cryptography, quantum computation, quantum encryption algorithm, unitary operator, Pauli matrices, algorithm works

INTRODUCTION

Cryptography or cryptology is a science to constructing and analyzing protocols that prevent eavesdropper from interpretation private messages. An algorithm called a cryptosystem or cipher works with the key to achieve this goal.

Classical cryptosystem can be generally divided into two types depending on the key. Where the sender and the receiver use the same key called symmetrical cipher for instance the Vernam algorithm (one time pad) (Schneier, 2007). When the sender and receiver use different key called asymmetric cipher. In this case, the security is based on complex computational for instance RSA algorithm (Rivest *et al.*, 1978).

Quantum cryptography is a science comes from the birth of the idea of quantum computation, it was clear that the nature of quantum measurement plays an important role in the secure transmission of information. So, it is obvious that one of the first significant contributions to quantum cryptography would be a way to prevent eavesdropping. The BB84 protocol proposed by Charles and Brassard (1984) allows secure quantum key distribution over an insecure channel and its experimentally demonstrated in 1992 (Bennett *et al.*, 1992).

There are many aspects of quantum cryptography proposed related to information security. We would like to refer to the quantum encryption algorithm proposed by Zhou *et al.* (2006) where a classical plaintext message is encrypted using a quantum computational algorithm employing 6 quantum keys divided into 4 groups. The output is a quantum ciphertext composed of 3 qubits. So, in this algorithm a classical bit is encrypted into 3 qubits. Moreover, we would like to refer to the algorithms (Run and Hua, 2005; Zeng, 2004; Cao and Liu, 2010; Abdullah *et al.*, 2016a). All of them in common can apply under certain circumstances self-inverse unitary operations to a message to encrypt a message. Other encryption algorithms like (Leung, 2002) are relying on entanglement where the entangled key is sent over an insecure quantum channel. A generalization by Leung (2002) is proven by Boykin and Roychowdhury (2003). Furthermore by Boykin and Roychowdhury (2003), a classical binary bit are encrypted using keys in a non-orthogonal quantum state which was extended by Leung (2002) to a new quantum encryption algorithm. Zhou *et al.* (2007), proposed standard one-time pad encryption algorithm for classical messages without a pre-shared or stored key. Khalaf and Abdullah (2014) proposed a novel quantum encryption algorithm that can be used to encrypt classical messages based on quantum shift register. Recently, Abdullah *et al.* (2015) presented a new protocol where this protocol work relies on the principle of the classical three-pass protocol and the properties of quantum mechanism and this is open new field to develop the quantum encryption algorithm (Abdullah *et al.*, 2015). In this study, we used the same concepts adopted by Zhou *et al.* (2006), Run and Hua (2005), Khalaf and Abdullah (2014), Abdullah *et al.* (2015, 2016b), Boykin and Roychowdhury (2003) and Ambainis *et al.* (2000) but we tend to utilize a novel scheme.

The sender takes a qubit to perform an operation on the qubit depending on the key. Then, the receiver applies some other transformation depending on the key such as ending up with the qubit. These operations represented as a four distinct unitary operators of Pauli matrices are generated using the property that every unitary operator can be written as a product of unitary operators under certain conditions.

Unitary operators: Unitary operators form the foundation of the encryption algorithm is presented in this study. Unitary operators can be written in the form:

$$U = e^{i\alpha} R_1(\beta) R_m(\gamma) R_1(\delta) \quad (1)$$

where, $R_\lambda(\xi) = e^{i\sigma\lambda\xi}$ and σ_λ being the Pauli matrices α, β, γ and δ are real numbers. Or alternatively we can write every unitary operator as:

$$U = e^{i\alpha} A \times B \times C, \text{ with } ABC = I \quad (2)$$

where A, B, C are unitary operators satisfying ABC = I. If we apply the unitary operator U to state $|\psi\rangle$ which means quantum message state, this leads to obtain the state $U|\psi\rangle$ which has density operator $U\,|\psi\rangle\langle\psi|U^\dagger$ (Kaye *et al.*, 2007).

MATERIALS AND METHODS

Pauli matrices: The Pauli matrices σ_x, σ_y and σ_z correspond to rotations about the x, y and z-axes of the Bloch sphere, respectively. The Pauli matrices are considered very important to the quantum computing and quantum cryptography because they span the vector space formed by all 1-qubit operators. In particular, this means that any 1-qubit unitary operators can be expressed as a linear combination of the Pauli gates.

For instance if we take the Pauli σ_x gate as an example where every 1-qubit pure state is represented as a point on the surface of the Bloch sphere or equivalently as a unit vector whose origin is fixed at the center of the Bloch sphere. A 1-qubit quantum gate U transforms a quantum state $|\psi\rangle$ into another quantum state $U\,|\psi\rangle$. In terms of the Bloch sphere, the action of U on $|\psi\rangle$ can be thought of as a rotation of the Bloch vector for $|\psi\rangle$ to the Bloch vector for $U\,|\psi\rangle$. For example, the not gate takes the state $|0\rangle$ to the state $|1\rangle$ (and takes $|1\rangle$ to $|0\rangle$). In terms of the Bloch sphere, this action can be visualized as a rotation through an angle π about the x-axis as illustrated in Fig. 1.

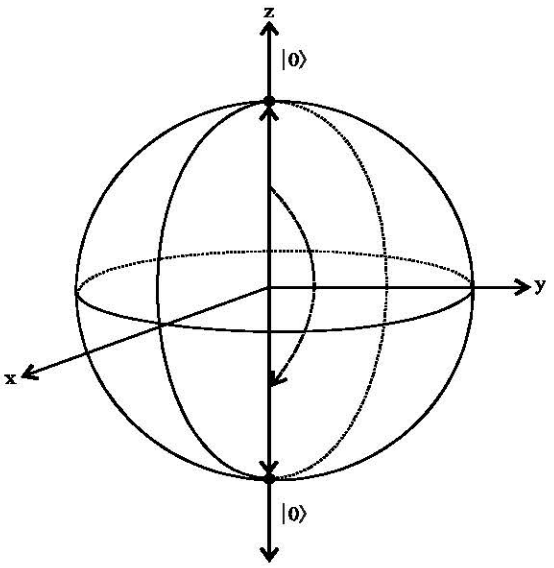

Fig. 1: Rotating the state $|0\rangle$ to the state $|1\rangle$ (Kaye *et al.*, 2007)

In this study, we used these rotation gates which correspond to rotations about the x, y and z-axes of the Bloch sphere. They are defined in terms of the Pauli matrices where defined as follows:

$$\mathbb{I} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \sigma_x \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \sigma_y \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \sigma_z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (3)$$

Quantum block encryption algorithm based on Pauli matrices: The idea of the algorithm is straightforward. As for the encryption of each qubit, we need one Pauli unitary operator, therefore, one out of four generated distinct Pauli unitary operators is selected according to the bit sequence of the measured quantum keys as described below. Thus, we split the Pauli unitary operator into three groups as follows:

The first group is ($\mathbb{I}$, σ_x, σ_y and σ_x, σ_y) the second group is ($\mathbb{I}$, σ_x, σ_z and σ_x, σ_z) and the third group is ($\mathbb{I}$, σ_y, σ_z and σ_y, σ_z). The groups of the operators allows us to change the algorithm whenever it is necessary where the sender and receiver agree about only one group to use it in the encryption algorithm where the encryption algorithm is designed based on these operators.

Quantum encryption: The idea for the Quantum Encryption Algorithm (QEA) is very obvious. We will use the same principle as in the superdense coding presented by Bennett and Wiesner (1992). Based on the combination

Table 1: Correspondence table for encryption

K_0, K_1	$U_{\gamma\mu}$
(0, 0)	U_{00}
(0, 1)	U_{01}
(1, 0)	U_{10}
(1, 1)	U_{10}

Table 2: Correspondence table for decryption

K_0, K_1	$U_{\gamma\mu}^{-1}$
(0, 0)	U_{00}^{-1}
(0, 1)	U_{01}^{-1}
(1, 0)	U_{10}^{-1}
(1, 1)	U_{11}^{-1}

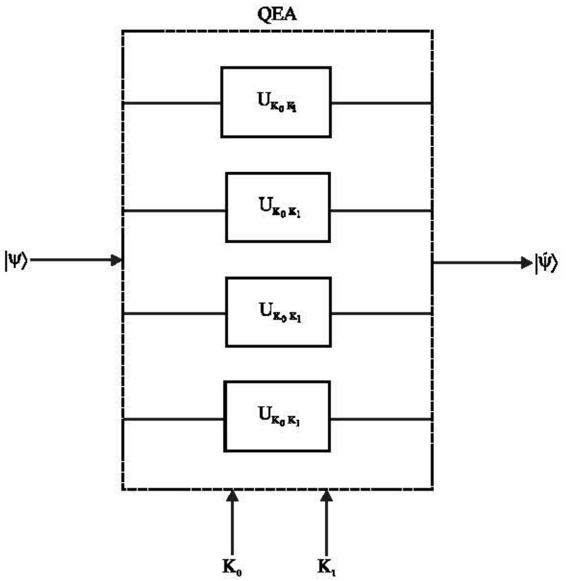

Fig. 2: Quantum block of encryption algorithm

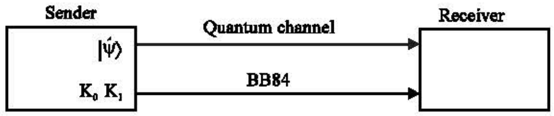

Fig. 3: Transmission of the quantum ciphertext and the keys

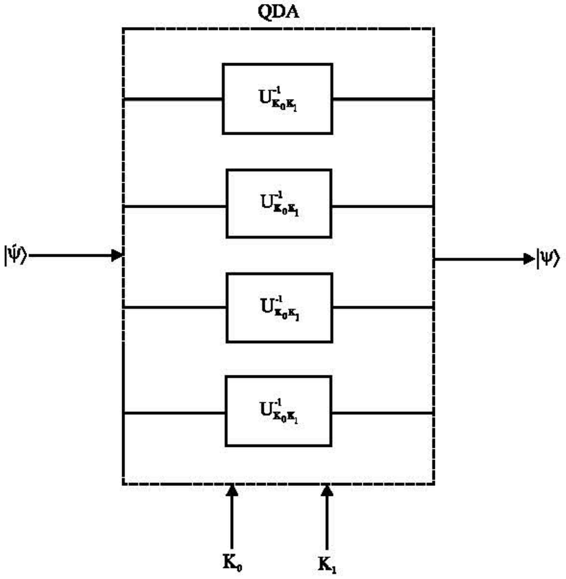

Fig. 4: Quantum block of decryption algorithm

of the two measured key bits K_0K_1, we will select the operation on $|\psi\rangle$. As we have two key bits of consideration, we can obtain four different combinations of these two bits. So, for each of the combination there must be a unique Pauli unitary operator assigned, i.e., $U_{\gamma\mu} \neq U_{ij}$ if $\gamma \neq i$ and $\mu \neq j$ resulting in Table 1.

For instance let $K_1 = 0$, $K_2 = 1$, $|\psi\rangle = |1\rangle$. Then, we compare the pair $(K_0, K_1) = (0, 1)$ with the bit pairs in Table 1, to assign the unitary operation U_{01} to encrypt $|\psi\rangle$. Finally, we apply the following operation on $|\psi\rangle$:

$$|\psi'\rangle = U_{10}|\psi\rangle \tag{4}$$

Resulting in the quantum ciphertext of the two key bits as shown in Fig. 2.

Transmission: We transmit the two keys K_0 K_1 using a quantum channel by BB84 protocol. After the sender and the receiver agree about the group that they use it in the quantum encryption algorithm in Fig. 3 and then the output of the algorithm is a quantum ciphertext $|\tilde{\psi}\rangle$ send to the receiver over a quantum channel as shown in Fig. 3.

Decryption: The idea for the Quantum Decryption Algorithm (QDA) is the same of quantum encryption algorithm but with opposite direction. Where it is based on the combination of the two key bits K_0 and K_1 that, we received by secure quantum channel, we will select the operation on $|\tilde{\psi}\rangle$. As we have two bits of consideration, we can have four different combinations of these two bits. So, for each of the combination there must be a unique inverse unitary operation assigned, i.e, $U^{-1}_{\gamma\mu} \neq U_{ij}$ if $\gamma \neq i$ and $\mu \neq j$ resulting in Table 2.

At the end, we apply the quantum cipher text $|\tilde{\psi}\rangle$ to the inverse of the unitary to get the quantum state message $|-\psi\rangle$ as shown in Fig. 4.

RESULTS AND DISCUSSION

Security analysis and algorithm optimization: First of all, it is preferable to have a look on what a quantum encryption algorithm scheme look like. Where the sender's goal is to send a qubit $||-\psi\rangle$ to the receiver via. quantum channel and the opponent trying to listen and intercept the qubit $|-\psi\rangle$. The keys that are used by sender

Table 3: Correspondence table for first group of Pauli operator

K_0, K_1	$U_{\gamma\mu}$
(0, 0)	$U_{00} = I$
(0, 1)	$U_{01} = X$
(1, 0)	$U_{10} = Z$
(1, 1)	$U_{11} = XZ$

and receiver are distributed by BB84 protocol. As in the output of the encryption algorithm $|\tilde{\psi}\rangle$ sends by the sender to the receiver. The opponent sees some state going across. The receiver needs a decryption function as the receiver apply some Pauli operators depending on the key such as ending up with $|-\psi\rangle$ eventually. So, to approve that our proposed algorithm is working perfectly, we should realized two conditions: first, the sender encrypt the qubits and the receiver can recover it. Second, it is secure which means that the state ρ that opponent sees is independent of $|-\psi\rangle$.

In order to fulfill the two conditions, we start to check whether the proposed algorithm is correct or not in other words the sender can recover the qubit unlike the opponent, the sender knows the key and hence he can simply apply the inverse of the Pauli operator operation that the sender performed. For the second condition, the proposed algorithm is secure. In other words, the state ρ that the opponent sees is independent of the message qubit. So, by using the density matrix formalism, we approved that the proposed algorithm is secure and the encrypted qubit $|-\tilde{\psi}\rangle$ is completely independent of the message qubit state $|\psi\rangle$. If we use for instance the first group of the Pauli operator's ($\mathbb{I}$, σ_x, σ_y and σ_x, σ_y) with two bits of key K_0, K_1 and quantum message state $|\psi\rangle$, if the key bits K_0K_1 = 00, we will apply. If, we utilize the K_0 K_1 = 01, we will apply X to message state $|\psi\rangle$. If, we used the K_0K_1 = 10, we apply Z to message state $|\psi\rangle$. Finally, if we adopt the K_0K_1 = 11, we will apply XZ to message state $|\psi\rangle$ as shown in Table 3.

Now, if we average out all of these four cases we, thus, see the density matrix ρ that the opponent see the state averaged over the two key bits. Therefore, it is just maximally mixed state (the identity) independent of the message state $|\psi\rangle$ (Kaye *et al*., 2007).

By the same way, we can approve that with the second and third group of Pauli operators, we see that the encryption state is independent of the initial qubit, the state that the opponent has is maximally mixed and the opponent cannot gain any information about the message state $|\psi\rangle$. So, the second condition approved as well.

Analysis of proposed algorithm: In the following example, we discuss how our algorithm works where the sender and receiver agree about the group of the Pauli operator which is for instance second group ($\mathbb{I}$ σ_x, σ_z and σ_x, σ_z) and the message qubit $|\psi\rangle = |-\rangle$, so, we encrypt the state based on the two key bits K_0 K_1 by applying the Pauli operator as in Table 4.

Table 4: Results table for quantum encryption

K_0, K_1	$U_{\gamma\mu}$	$\|\tilde{\psi}\rangle = U_{\gamma\mu}\|\psi\rangle$
(0, 0)	$U_{00} = I$	$I. \|-\rangle = \|-\rangle$
(0, 1)	$U_{01} = X$	$X. \|-\rangle = -\|-\rangle$
(1, 0)	$U_{10} = Z$	$Z. \|-\rangle = \|+\rangle$
(1, 1)	$U_{11} = XZ$	$XZ. \|-\rangle = \|+\rangle$

Table 5: Results of density matrix ρ

$U_{\gamma\mu}$	$\|\tilde{\psi}\rangle = U_{\gamma\mu}\|\psi\rangle$	ρ
$U_{00} = I$	$I. \|-\rangle = \|-\rangle$	$\|-\rangle\langle-\|$
$U_{01} = X$	$X. \|-\rangle = -\|-\rangle$	$X.-\rangle\langle-\|.X$
$U_{10} = Z$	$Z. \|-\rangle = \|+\rangle$	$Z.-\rangle\langle-\|.Z$
$U_{11} = XZ$	$XZ. \|-\rangle = \|+\rangle$	$XZ.-\rangle\langle-\|.XZ$
The averagge		$\frac{1}{4}\sum_{K_0K_1} U_{\psi\mu}\rho\, U_{\psi\mu}^{-1} = \frac{1}{2}$

Table 6: Results table for quantum decryption

K_0, K_1	$U_{\gamma\mu}$	$\|\psi\rangle = U_{\gamma\mu}^{-1}\|\tilde{\psi}\rangle$
(0, 0)	$U_{00} = I$	$\|-\rangle.I = \|-\rangle$
(0, 1)	$U_{01} = X$	$-\|-\rangle.X = \|-\rangle$
(1, 0)	$U_{10} = Z$	$\|+\rangle.Z = \|-\rangle$
(1, 1)	$U_{11} = XZ$	$\|+\rangle.ZX = \|-\rangle$

Now, if we compute the density matrix ρ which the opponent sees and average all out all of these output of encryption we get the maximally mixed state (the identity) as in Table 5.

The receiver makes the quantum decryption process where all the quantum encryption processes are inverted to get the final quantum message state $|\psi\rangle$ as shown in Table 6.

Finally, we get the quantum message state and proposed quantum encryption algorithm based on Pauli operator.

CONCLUSION

The quantum technology is very important and being improved continuously, especially in the field of quantum cryptography. At the same time, most of the world is challenging the fact that science and technology is in constant progress and sooner or later, the quantum computers will take their part in this world. So, it is not possible to treat or transfer all of the existing information in classical form which is more conventional to the people in quantum and pre-shared classical technology since the security cannot be guaranteed. Therefore, we present a quantum encryption algorithm based on Pauli operator in this study, we improved the quantum encryption algorithm, entailing two key bits to encrypt one quantum message state. The algorithm saves about half the time without the loss of the security.

RECOMMENDATIONS

The security is further improved through using the Pauli unitary operator where the sender and receiver agree about which Pauli operator group to be use before the encryption process begins where one does not know the key. The output is completely independent of the input which means, we have managed to hide all possible information from the opponent. This makes the algorithm probabilistic rather than deterministic.

REFERENCES

Abdullah, A.A., R.Z. Khalaf and M. Riza, 2016a. A modifiable 2-qubit quantum block encryption algorithm. Intl. J. Soft Comput., 11: 476-483.

Abdullah, A.A., A.M.A. Salih and A.K. Bermani, 2016b. A new quantum block encryption algorithm based on quantum key generation. Res. J. Appl. Sci., 11: 953-958.

Abdullah, A.A., R. Khalaf and M. Riza, 2015. A realizable quantum three-pass protocol authentication based on hill-cipher algorithm. Math. Prob. Eng., 2015: 1-6.

Ambainis, A., M. Mosca, A. Tapp and R.D. Wolf, 2000. Private quantum channels. Proceedings of the 41st Annual Symposium on Foundations of Computer Science, November 12-14, 2000, IEEE, Redondo Beach, California, ISBN: 0-7695-0850-2, pp: 547-553.

Bennett, C.H. and S.J. Wiesner, 1992. Communication via. one-and two-particle operators on einstein-podolsky-rosen states. Phys. Rev. Lett., 69: 2881-2884.

Bennett, C.H., F. Bessette, G. Brassard, L. Salvail and J. Smolin, 1992. Experimental quantum cryptography. J. Cryptol., 5: 3-28.

Boykin, P.O. and V. Roychowdhury, 2003. Optimal encryption of quantum bits. Phys. Rev. A, Vol. 67.

Cao, Z. and L. Liu, 2010. Improvement of one quantum encryption scheme. Proceedings of the 2010 IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS), October 29-31, 2010, IEEE, New York, USA., ISBN:978-1-4244-6585-9, pp: 335-339.

Charles, H.B. and G. Brassard, 1984. Quantum cryptography: Public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, System and Signal Processing, December 10-12, 1984, IEEE, Bangalore, India, pp: 175-179.

Kaye, P., R. Laflamme and M. Mosca, 2007. An Introduction to Quantum Computing. University Press, Oxford, ISBN: 0198570007, pp: 274.

Khalaf, R.Z. and A.A. Abdullah, 2014. Novel quantum encryption algorithm based on multiqubit quantum shift register and hill cipher. Adv. High Energy Phys., Vol. 2014,

Leung, D., 2002. Quantum vernam cipher. Quantum Inf. Comput., 2: 14-34.

Rivest, R.L., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM., 21: 120-126.

XRun, Z.N. and Z.G. Hua, 2005. A realizable quantum encryption algorithm for qubits. Chin. Phys., 14: 2164-2164.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithms and Source Code in C. 2nd Edn., John Wiley and Sons, New Delhi, India, ISBN-13: 9788126513680, Pages: 784.

Zeng, G.H., 2004. Encrypting binary bits via quantum cryptography. Chin. J. Electron., 13: 651-653.

Zhou, N., G. Zeng, Y. Nie, J. Xiong and F. Zhu, 2006. A novel quantum block encryption algorithm based on quantum computation. Phys. Stat. Mech. Appl., 362: 305-313.

Zhou, N., Y. Liu, G. Zeng, J. Xiong and F. Zhu, 2007. Novel qubit block encryption algorithm with hybrid keys. Phys. A. Stat. Mech. Appl., 375: 693-698.